

# PSEUDO-UNITARY NON-SELF-DUAL FUSION CATEGORIES OF RANK 4

HANNAH K. LARSON

**ABSTRACT.** A fusion category of rank 4 has either four self-dual simple objects or exactly two self-dual simple objects. We study fusion categories of rank 4 with exactly two self-dual simple objects, giving nearly a complete classification of those based rings that admit pseudo-unitary categorification. More precisely, we show that if  $\mathcal{C}$  is such a fusion category, then its Grothendieck ring  $K(\mathcal{C})$  must be one of seven based rings, six of which have known categorifications. In doing so, we classify all based rings associated with near-group categories of the group  $\mathbb{Z}/3\mathbb{Z}$ .

## 1. INTRODUCTION

A *fusion category* is a semi-simple rigid tensor category with finitely many simple objects such that the unit object is simple. A complete classification of fusion categories is considered out of reach (it would include the classification of all finite groups), but classification results have been reached in small cases. One notion of a “small” fusion category is a category with a small number of simple objects or *rank*. The only fusion category of rank 1 is the category of vector spaces. Fusion categories of rank 2 and rank 3 were classified in [11] and [9] respectively. Modular tensor categories (fusion categories with some additional structure) of rank 4 were classified in [12], and non-self-dual modular tensor categories of rank 5 were classified in [5]. In a fusion category of rank 4, either all four simple objects are self-dual, or exactly two simple objects are self-dual. Here, we study fusion categories of rank 4 with exactly two self-dual simple objects.

One approach to the problem of classifying fusion categories is to study related objects called based rings. A *based ring*, in the sense of [7], is a ring with a basis  $\mathbf{1} = X_0, X_1, X_2, \dots$  over  $\mathbb{Z}$  such that the coefficients  $N_{ij}^k$ , known as the *structure constants*, which appear in the decompositions  $X_i X_j = \sum_k N_{ij}^k X_k$  are nonnegative integers, and there exists an involution  $i \mapsto i^*$  such that  $N_{ij}^0 = \delta_{ij^*}$ . The following multiplication table describes a based ring of rank 4 with basis elements  $\mathbf{1}, X, Y$  and  $Z$ :

$\cdot$	$\mathbf{1}$	$X$	$Y$	$Z$
$\mathbf{1}$	$\mathbf{1}$	$X$	$Y$	$Z$
$X$	$X$	$Y + 2Z$	$2X + 2Y + Z$	$\mathbf{1} + 2Y$
$Y$	$Y$	$2X + 2Y + Z$	$1 + 2X + 4Y + 2Z$	$X + 2Y + 2Z$
$Z$	$Z$	$\mathbf{1} + 2Y$	$X + 2Y + 2Z$	$2X + Y$

TABLE 1. A Based Ring of Rank 4

The Grothendieck ring of a fusion category is a based ring. For example, the condition that there exists an involution  $i \mapsto i^*$  such that  $N_{ij}^0 = \delta_{ij^*}$  is motivated by the duality in a fusion category: if  $\mathcal{C}$  is a rigid category with duality functor  $A \mapsto A^*$ , then for any simple object  $X$ , the simple object  $\mathbf{1}$  appears exactly once in the decomposition  $X \otimes X^*$ .

An isomorphism of a based ring with the Grothendieck ring of a fusion category is called a *categorification* of the based ring. We say a based ring  $K$  is *pseudo-unitary categorifiable* if there exists a pseudo-unitary category  $\mathcal{C}$  such that  $K \simeq K(\mathcal{C})$ . There are many restrictions that pseudo-unitary categorifiable based rings are known to satisfy. For example, by Theorem 2.21 of [9], the *formal codegrees*  $f_0 \geq f_1 \geq \dots \geq f_{n-1}$  of a pseudo-unitary fusion category must satisfy  $\sum 1/f_i^2 \leq (1/2)(1+1/f_0)$ . Here, if the matrices for multiplication by basis elements of the based ring are  $\mathbf{1} = X_0, X_1, \dots, X_{n-1}$ , the formal codegrees of the based ring are the eigenvalues of the matrix  $M = 1 + X_1 X_1^* + X_2 X_2^* + \dots + X_{n-1} X_{n-1}^*$ . For example, the formal codegrees of the based ring in table 1, are  $36 + 20\sqrt{3}, 36 - 20\sqrt{3}, 8, 8$  which do not satisfy  $\sum 1/f_i^2 \leq (1/2)(1 + 1/f_0)$ . Hence, the based ring in table 1 has no pseudo-unitary categorifications.

As the above example shows, not all based rings have categorifications. In fact, from known examples it seems that the majority of based rings are not categorifiable. In this paper, we show that of the based rings of rank four with two self-dual basis elements (based rings whose involution fixes exactly two elements), at most seven are pseudo-unitary categorifiable. Of these seven, six have known categories associated with them.

The main theorems of this paper show the following:

**Theorem 1.1.** *Let  $K$  be a based ring of rank four with basis  $\mathbf{1}, X, Y, Z$ , where  $X$  and  $Z$  are duals of each other and  $Y$  is self-dual. If  $K$  is pseudo-unitary categorifiable then  $K$  is one of the following:*

- (1) the Grothendieck ring of the Tambara-Yamagami category associated with  $\mathbb{Z}/3\mathbb{Z}$  [14]
- (2) the Grothendieck ring of the category of representations of the alternating group  $A_4$
- (3) the Grothendieck ring of the Izumi-Xu category [3]
- (4) the based ring with multiplication given by

$$\begin{array}{lll} X^2 = Z & Y^2 = 1 + X + 6Y + Z & Z^2 = X \\ XY = YX = Y & YZ = ZY = Y & XZ = ZX = 1. \end{array}$$

- (5) the Grothendieck ring of the category of representations of  $\mathbb{Z}/4\mathbb{Z}$
- (6) the based ring with multiplication given by

$$\begin{array}{lll} X^2 = cX + Y + cZ & Y^2 = \mathbf{1} & Z^2 = cX + Y + cZ \\ XY = YX = Z & YZ = ZY = X & XZ = ZX = \mathbf{1} + cX + cZ \end{array}$$

where  $c = 1$  or  $2$ .

*Remark 1.2.* It was shown recently by Zhengwei Liu and Noah Snyder that the based ring in (4) is categorifiable. It was pointed out by Scott Morrison that the based ring in (6) with  $c = 1$  is also categorifiable via (the even part of) the subfactor  $\mathcal{S}'$  from [6] Theorem 1. A recent paper of Bruillard shows that only (2) and (5) have associated categories with a ribbon structure [2].

The proofs of the main theorems rely on results bounding the minimum number of roots of unity required to write certain quadratic irrationalities as sums of roots of unity. For example, we prove the following in section 6:

**Theorem 1.3.** *Let  $a, b, c \in \mathbb{Z}$  with  $c$  nonnegative and square free. If there exist  $n$  roots of unity  $\theta_i$  such that  $\sum_{i=0}^n \theta_i = a + b\sqrt{c}$ , then  $n \geq |b|\varphi(2c)$ .*

This paper is organized as follows. In section 2, we parameterize based rings of rank 4 with two self-dual basis elements. In section 3, we find that if  $K$  is pseudo-unitary categorifiable, then it belongs to one of two one-parameter families. One of these families is associated with the near-group categories of  $\mathbb{Z}/3\mathbb{Z}$ . We study each of these families separately in sections 4 and 5 by assuming there exists a category  $\mathcal{C}$  with  $K(\mathcal{C})$  in the family, computing information about the Drinfeld center  $\mathcal{Z}(\mathcal{C})$ , and taking traces of balance isomorphisms. This gives us identities for the twists that can only be satisfied when the free parameter is small. These identities involve sums of twists, which are roots of unity, equaling certain quadratic irrationalities. Thus, we need tight bounds on how many roots of unity it takes to write these quadratic irrationalities. We refer to these bounds in sections 4 and 5 but delay their proofs to section 6.

## 2. EXPLICIT PARAMETERIZATION OF BASED RINGS

In this section, we parameterize based rings of rank four with two self-dual basis elements in terms of some diophantine equations and then solve these equations to reduce the number of parameters necessary to describe the based rings.

Let  $c, e, k, l, p, q$  be nonnegative integers subject to the conditions

$$\begin{aligned} (1) \quad & kl + lc = lp + kq \\ (2) \quad & kp + le + kc = 2lq + k^2 \\ (3) \quad & l^2 + c^2 = 1 + q^2 + p^2 \\ (4) \quad & l^2 + k^2 + q^2 = 1 + 2pk + qe. \end{aligned}$$

Let  $K(c, e, k, l, p, q)$  be the based ring with the basis  $\mathbf{1}, X, Y, Z$  and multiplication given by

$$\begin{aligned} X^2 &= pX + lY + cZ & XY &= YX = qX + kY + lZ \\ Y^2 &= 1 + kX + eY + kZ & YZ &= ZY = lX + kY + qZ \\ Z^2 &= cX + lY + pZ & XZ &= ZX = 1 + pX + qY + pZ. \end{aligned}$$

The following classifies based rings of rank four with exactly two self-dual basis elements.

**Proposition 2.1.** *Let  $K$  be a based ring of rank 4 with exactly two self-dual basis elements. Then  $K = K(c, e, k, l, p, q)$  for some nonnegative integers  $c, e, k, l, p, q$  satisfying (1)–(4).*

*Proof.* We first observe that any based ring of rank 4 is commutative. The complexification of  $K$  is isomorphic to a direct sum of matrix algebras over the complex numbers. Because we are in rank 4, the complexification is isomorphic to either two-by-two matrices over  $\mathbb{C}$  or  $\mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}$ . Since we have a non-trivial homomorphism into the complex numbers, namely sending each object to its dimension, we must be in the latter case, so  $K$  is commutative.

Working in the basis  $\mathbf{1}, X, Y, Z$ , the general matrices for left multiplication in the commutative ring where  $\mathbf{1}$  and  $Y$  are the only self-dual basis elements are

$$M_X = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & p & q & p \\ 0 & l & k & q \\ 0 & c & l & p \end{pmatrix}, \quad M_Y = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & q & k & l \\ 1 & k & e & k \\ 0 & l & k & q \end{pmatrix}, \quad M_Z = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & p & l & c \\ 0 & q & k & l \\ 1 & p & q & p \end{pmatrix}.$$

The repeated identical columns come from commutativity, the zeros and ones of the first column are determined by  $\mathbf{1}$  being a unit, and the zeros and ones of the first row are determined by duality. We know  $M_Y$  must be symmetric because  $Y$  is self-dual. Also,  $M_X = M_Z^\dagger$  because  $X$

is the dual of  $Y$ . Commutativity of  $K$  implies the above matrices commute, which gives us the restrictions (1)–(4).  $\square$

We now reduce the number of parameters needed to describe these based rings from six to four by reformulating the restrictions (1)–(4).

**Definition 2.2.** Let  $x, y, g, d$  be integers satisfying

$$(5) \quad yg + xd + y \equiv 0 \pmod{2},$$

$$(6) \quad dxy = g(2x^2 - y^2) + x^2 + 1,$$

and  $\frac{yg+xd+y}{2}, 2xg - yd + 2x, gy, gx, \frac{yg+xd-y}{2}, xg + x \geq 0$ . We define

$$R(x, y, g, d) = K \left( \frac{yg + xd + y}{2}, 2xg - yd + 2x, gy, gx, \frac{yg + xd - y}{2}, xg + x \right).$$

The reader can check that the condition  $dxy = g(2x^2 - y^2) + x^2 + 1$  implies (1)–(4). Note that if integers  $x, y, g, d$  satisfy these restrictions, then  $-x, -y, -g, -d$  satisfy them as well. Also note that  $xg \geq 0$  and  $yg \geq 0$  implies either both  $x, y \leq 0$  or both  $x, y \geq 0$ .

**Proposition 2.3.** Any based ring  $K(c, e, k, l, p, q)$  is of the form  $R(x, y, g, d)$  for integers  $x, y, g, d$ , with  $(x, y) = 1$ .

*Proof.* Given  $K(c, e, k, l, p, q)$ , there exist  $g, x$ , and  $y$  such that  $l = gx$  and  $k = gy$  with  $(x, y) = 1$ . Rewriting (1) in terms of  $g, x$ , and  $y$  we find  $x(gy + c - p) = yq$  which implies  $x \mid q$  and  $y \mid c - p$ . Let  $q = ax$  and  $c - p = by$ . Then (1) gives  $g + b = a$ . Similarly, (2) implies  $x \mid p + c - gy$  and  $y \mid 2q - e$ . Let  $p + c - gy = dx$  and  $2q - e = fy$ . Then (2) gives  $d = f$ . We write  $c, e, k, l, p, q$  as

$$(7) \quad c = (dx + gy + by)/2 \quad e = 2(g + b)x - dy \quad k = gy$$

$$(8) \quad l = gx \quad p = (dx + gy - by)/2 \quad q = (g + b)x$$

Note that the equations for  $c$  and  $p$  imply the divisibility constraint (5). Finally, (3) and (4) give us  $(gx)^2 - 1 = (g + b)^2 x^2 - by(dx + gy)$ , or equivalently

$$(9) \quad dbxy = gb(2x^2 - y^2) + b^2 x^2 + 1.$$

As every term of (9) except 1 has a factor of  $b$ , we have  $b = \pm 1$ . If  $b = 1$ , (9) becomes (6), and  $K(c, e, k, l, p, q) = R(x, y, g, d)$ . If  $b = -1$ , then (9) becomes (6) for  $R(-x, -y, -g, -d)$ , and  $K(c, e, k, l, p, q) = R(-x, -y, -g, -d)$ .  $\square$

The following propositions give some additional information about the parameters  $x, y$  and  $g$ . The first gives a useful restriction on the parity of  $x$  and  $y$ .

**Proposition 2.4.** Let  $x, y, g, d$  be integers satisfying (5) and (6). Then  $x + y \equiv 1 \pmod{2}$ .

*Proof.* We use case work to get the following implications. First,

$dx$  and  $y(g + 1)$  both odd  $\Rightarrow d, x, y$  odd and  $g$  even  $\Rightarrow$  LHS of (6) is odd, RHS is even.  
Hence,  $2 \mid dx$  and  $2 \mid y(g - 1)$ . Next,

$$x \text{ is odd} \Rightarrow d \text{ is even} \Rightarrow 2 \mid gy^2 \Rightarrow \begin{cases} \text{either } gx \text{ is even} & \Rightarrow y \text{ is even} \\ \text{or } g \text{ is odd} & \Rightarrow y \text{ is even} \end{cases}$$

And,  $x$  is even  $\Rightarrow gy^2$  is odd  $\Rightarrow y$  is odd. Therefore,  $x + y \equiv 1 \pmod{2}$ .  $\square$

**Proposition 2.5.** *If  $R(x, y, g, d) = K(c, e, k, l, p, q)$  for  $c, e, k, l, p, q \in \mathbb{Z}_{\geq 0}$ , then  $g \neq 0$ .*

*Proof.* Assume  $g = 0$ . Then  $k = gy = 0$  and  $l = gx = 0$ . The restriction (4) gives  $e = 0$ , and  $q = 1$ . Then (3) gives  $c^2 = 2 + p^2$ , which is a contradiction. Hence  $g \neq 0$ .  $\square$

### 3. FIRST REDUCTIONS

In this section we show that if a based ring  $K(c, e, k, l, p, q)$  admits pseudo-unitary categorification, it belongs to one of two one-parameter families. Recall the matrices  $M_X$ ,  $M_Y$ , and  $M_Z$  for left-multiplication by basis elements:

$$M_X = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & p & q & p \\ 0 & l & k & q \\ 0 & c & l & p \end{pmatrix}, \quad M_Y = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & q & k & l \\ 1 & k & e & k \\ 0 & l & k & q \end{pmatrix}, \quad M_Z = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & p & l & c \\ 0 & q & k & l \\ 1 & p & q & p \end{pmatrix}$$

If  $A = 1 + M_Y^2 + 2M_X M_Z$ , then the *formal codegrees*  $f_1 \geq f_2, f_3, f_4$  are the roots of the characteristic polynomial of  $A$ . By Theorem 2.21 of [9], if  $K$  is pseudo-unitary categorifiable, the formal codegrees satisfy  $f_1, f_2, f_3, f_4 > 0$  and

$$(10) \quad \frac{1}{f_1^2} + \frac{1}{f_2^2} + \frac{1}{f_3^2} + \frac{1}{f_4^2} \leq \frac{1}{2} \left( 1 + \frac{1}{f_1} \right).$$

In addition, by Proposition 2.10 of [9], we have

$$(11) \quad \frac{1}{f_1} + \frac{1}{f_2} + \frac{1}{f_3} + \frac{1}{f_4} = 1.$$

We will see that the characteristic polynomial of  $A$  always factors over  $\mathbb{Q}$  as  $(t - \gamma)^2 \cdot (t^2 - \alpha t + \beta)$  for integers  $\gamma, \alpha, \beta$ . The following lemmas greatly restrict the possibilities for  $\gamma$ , which we will translate into restrictions on the parameters  $x$  and  $y$ .

**Lemma 3.1.** *Any polynomial of the form  $(t - \gamma)^2 \cdot (t^2 - \alpha t + \beta)$ , for integers  $\gamma, \alpha$ , and  $\beta$  with roots  $f_1 \geq f_2, f_3, f_4$  that satisfies (10), (11), and  $\beta \geq \gamma^2$ , must have  $2 < \gamma < 8$ .*

*Proof.* Expand  $(t - \gamma)^2 \cdot (t^2 - \alpha t + \beta) = t^4 + (-\alpha - 2\gamma)t^3 + (\beta + 2\gamma\alpha + \gamma^2)t^2 + (-\gamma^2\alpha - 2\gamma\beta)t + \gamma^2\beta$ . Consequently,

$$\begin{aligned} \frac{\gamma^2\alpha + 2\gamma\beta}{\gamma^2\beta} &= \frac{1}{f_1} + \frac{1}{f_2} + \frac{1}{f_3} + \frac{1}{f_4} = 1 \quad \Rightarrow \quad \frac{-\alpha}{\beta} = \frac{2}{\gamma} - 1. \\ \Rightarrow \frac{1}{f_1^2} + \frac{1}{f_2^2} + \frac{1}{f_3^2} + \frac{1}{f_4^2} &= \left( \frac{1}{f_1} + \frac{1}{f_2} + \frac{1}{f_3} + \frac{1}{f_4} \right)^2 - 2 \cdot \sum_{i \neq j} \frac{f_i f_j}{f_1 f_2 f_3 f_4} \\ &= 1^2 - 2 \cdot \frac{\beta + 2\gamma\alpha + \gamma^2}{\gamma^2\beta} \\ &= 1 - \frac{2}{\gamma^2} + \frac{4}{\gamma} \cdot \frac{-\alpha}{\beta} - \frac{2}{\beta} \\ &= 1 - \frac{2}{\gamma^2} + \frac{4}{\gamma} \cdot \left( \frac{2}{\gamma} - 1 \right) - \frac{2}{\beta} \\ &= 1 + \frac{6}{\gamma^2} - \frac{4}{\gamma} - \frac{2}{\beta}. \end{aligned}$$

Hence,  $1 + 6/\gamma^2 - 4/\gamma - 2/\beta \leq (1/2) \cdot (1 + 1/f_1)$ . Since  $\beta \geq \gamma^2$ , we have  $f_1 f_2 f_3 f_4 = \gamma^2 \beta \geq \gamma^4$ , so either there exists  $i$  such that  $f_i > \gamma$ , or  $f_i = \gamma$  for all  $i$ . In the latter case,  $\gamma = 4$  because of

condition (11). Otherwise,  $f_1 > \gamma$  implies  $\frac{1}{2}(1+1/f_1) < \frac{1}{2}(1+1/\gamma)$ . Using this, and  $2/\beta \leq 2/\gamma^2$ ,

$$1 + \frac{6}{\gamma^2} - \frac{4}{\gamma} - \frac{2}{\gamma^2} < \frac{1}{2} \left( 1 + \frac{1}{\gamma} \right) \Rightarrow \gamma < 8.$$

Also, by condition (11),  $\gamma > 2$ . □

**Lemma 3.2.** *If  $f_1, f_2, f_3, f_4$  are nonnegative integers with  $f_1 \geq f_2 \geq f_3 \geq f_4$  and  $f_i = f_j$  for some  $i \neq j$  satisfying (11) then  $(f_1, f_2, f_3, f_4)$  is one of the following*

$$\begin{array}{cccc} (12, 12, 3, 2) & (8, 8, 4, 2) & (10, 5, 5, 2) & (6, 6, 6, 2) \\ (6, 6, 3, 3) & (6, 4, 4, 3) & (12, 4, 3, 3) & (4, 4, 4, 4) \end{array}$$

*Proof.* We begin by considering the case when  $f_4 = 2$ . Clearly,  $f_3 \neq 2$ . If  $f_3 = 3$  then we must have  $f_2 = f_1 = 12$ ; if  $f_3 = 4$ , then  $f_2 \neq 4$  so we must have  $f_2 = f_1 = 8$ ; if  $f_3 = 5$ , either  $f_2 = 5 \Rightarrow f_1 = 10$ , or  $f_2 = f_1 \Rightarrow 2/f_2 = 1 - 1/2 - 1/5 = 3/10 \Rightarrow f_2 = 20/3$ , a contradiction; if  $f_3 = 6$ , we must have  $f_2 = f_3$  or  $f_2 = f_1$ , both of which imply  $(f_1, f_2, f_3, f_4) = (6, 6, 6, 2)$ . If  $f_3 > 6$  then (11) is not satisfied.

Now consider  $f_4 = 3$ . If  $f_3 = 3$ , then  $1/f_2 + 1/f_1 = 1/3$ . We see  $f_2 = 4 \Rightarrow f_1 = 12$ ,  $f_2 = 5 \Rightarrow f_1 = 2/15$ , a contradiction,  $f_2 = 6 \Rightarrow f_1 = 6$ , and  $f_2 > 6 \Rightarrow f_2 > f_1$  another contradiction. If  $f_3 = 4$ , then  $f_2 = 4 \Rightarrow f_1 = 6$ , and  $f_2 = f_1 \Rightarrow 2/f_2 = 5/12 \Rightarrow f_2 = 5/6$ , a contradiction. For  $f_3 > 4$ , (11) fails.

Finally, if  $f_4 = 4$ , we must have  $f_4 = f_3 = f_2 = f_1$ . For  $f_4 > 4$ , there must exist some  $f_i < 4$  for (11) to be satisfied, which contradicts  $f_1 \geq f_2 \geq f_3 \geq f_4$ . □

**Theorem 3.3.** *Assume there exists a pseudo-unitary category  $\mathcal{C}$  such that  $K(\mathcal{C}) = K(c, e, k, l, p, q)$ . Then either  $K(\mathcal{C}) = K(c, 0, 0, 1, c, 0)$  or  $K(\mathcal{C}) = K(1, e, 1, 0, 0, 0)$ .*

*Proof.* Let  $x, y, g, d$  be integers such that  $K(c, e, k, l, p, q) = R(x, y, g, d)$ . Compute the characteristic polynomial  $P_A(t)$  of  $A = 1 + M_Y^2 + 2M_X M_Z$  in terms of  $x, y, g$ , and  $d$ . Let  $\gamma = 2x^2 + y^2 + 2$ . Evaluating  $P_A(\gamma)$  and  $P'_A(\gamma)$ , and factoring over  $\mathbb{Q}[x, y, g, d]$ , we get something divisible by (6). Thus,  $\gamma$  is a double root of  $P_A(t)$ , i.e.  $P_A(t) = (t - \gamma)^2 \cdot (t^2 - \alpha t + \beta)$  for integers  $\alpha$  and  $\beta$ .

We claim  $2 < \gamma < 8$ . If  $(t^2 - \alpha t + \beta)$  is irreducible,  $\gamma^2 \mid \beta$  by Corollary 2.14 of [9]. In particular,  $\gamma^2 \leq \beta$ , so Lemma 3.1 implies  $2 < \gamma < 8$ . If  $(t^2 - \alpha t + \beta)$  splits into two linear factors, then Lemma 3.2 implies  $\gamma = 3, 4, 5, 6, 8$ , or  $12$ . The cases that remain to be considered are  $\gamma = 12$ , and  $\gamma = 8$ . Since  $12$  cannot be written as  $2x^2 + y^2 + 2$  for integers  $x, y$ , we can't have  $\gamma = 12$ .

If  $\gamma = 8$ , the other two roots are  $2$  and  $4$ , by Lemma 3.2. The product of the four roots  $8 \cdot 8 \cdot 4 \cdot 2 = 512$  equals  $\det A$ . As  $\gamma = 8$ , we have  $(x, y) = (\pm 1, \pm 2)$ . In both cases,  $d = 1 - g$  by (6) and  $\det A = 4608g^2 + 1024g + 512$ . By Proposition 2.5,  $g \neq 0$ , so  $\det A > 512$ . Hence,  $\gamma \neq 8$ .

Since  $\gamma = 2x^2 + y^2 + 2$  for integers  $x, y$  satisfying

$$\begin{array}{ll} (x, y) = 1 & \text{by Proposition 2.3} \\ x + y \equiv 1 \pmod{2} & \text{by Lemma 2.4,} \end{array}$$

either  $(x, y) = (0, \pm 1)$  or  $(x, y) = (\pm 1, 0)$ . Using (9) and  $k, l \geq 0$ , we can determine  $g$  and  $b$ . Then using (7) and (8), we determine  $c, e, k, l, p, q$ . Note that  $d$  is a free parameter, which gives the based rings  $K(1, e, 1, 0, 0, 0)$  when  $(x, y) = (0, \pm 1)$ , and  $K(c, 0, 0, 1, c, 0)$  when  $(x, y) = (\pm 1, 0)$ . □

*Remark 3.4.* If  $K(1, e, 1, 0, 0, 0) = R(x, y, g, d)$ , then  $(x, y) = (0, \pm 1)$  and  $P_A(t)$  has a repeated root equal to 3, so two of the formal codegrees of  $K(1, e, 1, 0, 0, 0)$  are  $f_1 = f_2 = 3$ .

*Remark 3.5.* If  $K(c, 0, 0, 1, c, 0) = R(x, y, g, d)$ , then  $(x, y) = (\pm 1, 0)$  and  $P_A(t)$  has a repeated root equal to 4, so two of the formal codegrees of  $K(c, 0, 0, 1, c, 0)$  are  $f_1 = f_2 = 4$ .

For the remainder of this paper, we will write  $K_1(e)$  for  $K(1, e, 1, 0, 0, 0)$  and  $K_2(c)$  for  $K(c, 0, 0, 1, c, 0)$ . The remainder of the paper shows that  $K_1(e)$  can only admit categorification when  $e = 0, 2, 3, 6$ , and  $K_2(c)$  can only admit categorification when  $c = 0, 1, 2$ .

#### 4. CATEGORIFICATIONS OF $K_1(e)$

Throughout this section we will assume that  $\mathcal{C}$  is a fusion category with  $K(\mathcal{C}) \simeq K_1(e)$ . We study the Drinfeld center  $\mathcal{Z}(\mathcal{C})$ , which is a modular tensor category, to arrive at a contradiction when  $e$  is not equal to 0, 2, 3, 6. These values for  $e$  give rise to the based rings (1) - (4) respectively of Theorem 1.1. Recall that the multiplication of basis elements in  $K_1(e)$  is given by

$$\begin{aligned} X^2 &= Z & Y^2 &= 1 + X + eY + Z & Z^2 &= X \\ XY &= YX = Y & YZ &= ZY = Y & XZ &= ZX = 1. \end{aligned}$$

*Remark 4.1.*  $K_1(e)$  is the family of near-group categories associated with the group  $\mathbb{Z}/3\mathbb{Z}$ .

**4.1. Induction and Forgetful Functors.** Let  $F : \mathcal{Z}(\mathcal{C}) \rightarrow \mathcal{C}$  be the forgetful functor, and let the induction functor  $I : \mathcal{C} \rightarrow \mathcal{Z}(\mathcal{C})$  be its right adjoint. We will study the effect of  $I$  and  $F$  on  $K(\mathcal{C})$  and  $K(\mathcal{Z}(\mathcal{C}))$ . Propositions 4.3 and 4.4 describe the simple objects in  $\mathcal{Z}(\mathcal{C})$ , giving their images under  $F$  and their dimensions.

Let  $k = \frac{e}{3}$  and  $\delta = \frac{e + \sqrt{e^2 + 12}}{2} = \frac{3k + \sqrt{9k^2 + 12}}{2}$ .

**Proposition 4.2.** *The dimensions of simple objects in  $\mathcal{C}$  are  $\text{FPdim}(Y) = \delta$ , and*

$$\text{FPdim}(\mathbf{1}) = \text{FPdim}(X) = \text{FPdim}(Z) = 1.$$

*In particular,  $\dim(\mathcal{C}) = 6 + 3k\delta$ .*

*Proof.* Recall the matrix for left multiplication

$$M_Y = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & e & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

The characteristic polynomial of  $M_Y$  is  $t^2 \cdot (t^2 - et - 3)$ . Thus,  $\text{FPdim}(Y) = \frac{e + \sqrt{e^2 + 12}}{2} = \delta$ .

By the same method  $\text{FPdim}(\mathbf{1}) = \text{FPdim}(X) = \text{FPdim}(Z) = 1$ . We can now compute  $\dim(\mathcal{C}) = \text{FPdim}(\mathbf{1})^2 + \text{FPdim}(X)^2 + \text{FPdim}(Y)^2 + \text{FPdim}(Z)^2 = 1 + 1 + \delta^2 + 1 = 6 + 3k\delta$ .  $\square$

Note that  $\delta$  is irrational unless  $e = 2$ , in which case  $K_1(e)$  is the Grothendieck ring of the category of representations of the alternating group  $A_4$ , and so is already known to admit categorification. From now on, we will assume  $e \neq 2$ , and hence  $\delta$  is irrational.

**Proposition 4.3.** *There exist non-isomorphic simple objects in  $\mathbf{1}, A, B, C, D, E, G, H, J$  in  $\mathcal{Z}(\mathcal{C})$  for which*

$$I(\mathbf{1}) = \mathbf{1} \oplus A \oplus B \oplus C \quad I(X) = B \oplus D \oplus E \oplus G, \quad I(Z) = C \oplus D \oplus H \oplus J,$$

and

$$\begin{aligned}
F(A) &= \mathbf{1} \oplus kY & F(D) &= X \oplus \alpha Y \oplus Z & F(H) &= rY \oplus Z \\
F(B) &= \mathbf{1} \oplus X \oplus kY & F(E) &= X \oplus rY & F(J) &= pY \oplus Z \\
F(C) &= \mathbf{1} \oplus kY \oplus Z & F(G) &= X \oplus pY,
\end{aligned}$$

where  $r, p$  and  $\alpha$  are integers satisfying  $\alpha + r + p = 2k$ . In particular,

$$\begin{aligned}
\dim(A) &= 1 + k\delta & \dim(D) &= 2 + \alpha\delta & \dim(H) &= 1 + r\delta \\
\dim(B) &= 2 + k\delta & \dim(E) &= 1 + r\delta & \dim(J) &= 1 + p\delta \\
\dim(C) &= 2 + k\delta & \dim(G) &= 1 + p\delta.
\end{aligned}$$

*Proof.* By Theorem 2.13 of [9], since  $K_1(e)$  has 4 irreducible representations, the object  $I(\mathbf{1}) \in \mathcal{Z}(\mathcal{C})$  decomposes into the sum of 4 simple objects. Because

$$\dim \operatorname{Hom}(\mathbf{1}, I(\mathbf{1})) = \dim \operatorname{Hom}(F(\mathbf{1}), \mathbf{1}) = \dim \operatorname{Hom}(\mathbf{1}, \mathbf{1}) = 1,$$

one of these objects must be  $\mathbf{1}$ . So let  $I(\mathbf{1}) = \mathbf{1} \oplus A \oplus B \oplus C$ . Two of the formal codegrees of the based ring  $K_1(e)$  are  $f_1 = f_2 = 3$  (see Remark 3.4), so by Theorem 2.13 of [9], we can assume that  $\dim(B) = \dim(C) = \frac{\dim(\mathcal{C})}{3} = 2 + k\delta$ , whence  $\operatorname{FPdim}(A) = \frac{\dim(\mathcal{C})}{3} - 1 = 1 + k\delta$ . Consider  $F(I(\mathbf{1}))$ . We denote by  $\mathbb{O}(\mathcal{C})$  the set of isomorphism classes of simple objects of  $\mathcal{C}$ . By Proposition 5.4 of [4] we have

$$F(\mathbf{1}) \oplus F(A) \oplus F(B) \oplus F(C) = F(I(\mathbf{1})) = \bigoplus_{X \in \mathbb{O}(\mathcal{C})} X \otimes \mathbf{1} \otimes X^* = 4 \cdot \mathbf{1} \oplus X \oplus eY \oplus Z.$$

Let  $F(A) = \mathbf{1} \oplus lX \oplus mY \oplus nZ$ . Then,  $1 + k\delta = \dim(A) = 1 + l + m\delta + n$ . Since  $\delta \notin \mathbb{Q}$ , we have  $m = k$  and  $l + n = 0$ , so  $l = n = 0$ . Thus,  $F(A) = \mathbf{1} \oplus kY$ . We repeat the same arguments to determine  $F(B)$  and  $F(C)$ .

Next we consider  $I(X)$ . Using Proposition 5.4 of [4], we calculate

$$F(I(X)) = \bigoplus_{Y \in \mathbb{O}(\mathcal{C})} Y \otimes X \otimes Y^* = \mathbf{1} \oplus 4X \oplus 3kY \oplus Z.$$

Since  $\dim \operatorname{Hom}(I(\mathbf{1}), I(X)) = \dim \operatorname{Hom}(F(I(\mathbf{1})), X) = 1$ , the decompositions of  $I(X)$  and  $I(\mathbf{1})$  have exactly one simple object in common. As

$$\dim \operatorname{Hom}(B, I(X)) = \dim \operatorname{Hom}(F(B), X) = 1,$$

this object is  $B$ . Finally, as  $\dim \operatorname{Hom}(I(X), I(X)) = \dim \operatorname{Hom}(F(I(X)), X) = 4$ , we see  $I(X)$  is the sum of four simple objects. Thus, let  $I(X) = B \oplus D \oplus E \oplus G$ . We have

$$\begin{aligned}
(\mathbf{1} \oplus X \oplus kY) \oplus F(D) \oplus F(E) \oplus F(G) &= F(I(X)) = \mathbf{1} \oplus 4X \oplus 3kY \oplus Z \\
\Rightarrow F(D) \oplus F(E) \oplus F(G) &= 3X \oplus 2kY \oplus Z.
\end{aligned}$$

Since  $\dim \operatorname{Hom}(D, I(X)) = \dim \operatorname{Hom}(F(D), X) = 1$ , let  $F(D) = X \oplus \alpha Y \oplus \beta Z$ . By a similar argument,  $F(E) = X \oplus rY \oplus sZ$  and  $F(G) = X \oplus pY \oplus qZ$ , where  $\alpha + r + p = 2k$  and  $\beta + s + q = 1$ . Without loss of generality, we can assume  $\beta = 1$ , so  $s = q = 0$ .

Finally, since  $\dim \operatorname{Hom}(I(X), I(Z)) = \dim \operatorname{Hom}(F(I(X)), Z) = 1$ , the decompositions of  $I(Z)$  and  $I(X)$  have exactly one simple object in common. By duality, there are objects  $H = E^*$  and  $J = G^*$  for which  $I(Z) = C \oplus D \oplus H \oplus J$ , and  $F(H) = rY \oplus Z$  and  $F(J) = pY \oplus Z$ .  $\square$

Note that, under our assumption that  $e \neq 2$ , we have shown  $3 \mid e$ , i.e.  $k$  is an integer.



**Proposition 4.4.** *There exist simple objects  $L_i \in \mathcal{Z}(\mathcal{C})$  and positive integers  $\gamma_i$  such that*

$$I(Y) = kA + kB + kC + kD + rE + pG + rH + pJ + \sum \gamma_i L_i$$

*where the objects  $L_i$  satisfy  $F(L_i) = \gamma_i Y$  and  $\sum \gamma_i^2 = 6 + 5k^2 - 2(r^2 + p^2)$ .*

*Proof.* Consider  $F(I(Y))$ . We have

$$F(I(Y)) = \bigoplus_{X \in \mathcal{O}(\mathcal{C})} X \otimes Y \otimes X^* = 3k \oplus 3kX \oplus (6 + 9k^2)Y \oplus 3kZ.$$

Since  $I$  and  $F$  are adjoint, the multiplicity to which an object  $O$  appears in the decomposition of  $I(Y)$  equals the multiplicity of  $Y$  in  $F(O)$ . Thus by Proposition 4.3,

$$(12) \quad I(Y) = kA + kB + kC + kD + rE + pG + rH + pJ + \sum \gamma_i L_i$$

where the objects  $L_i$  satisfy  $F(L_i) = \gamma_i Y$ . Then,

$$\begin{aligned} k^2 + k^2 + k^2 + k^2 + 2r^2 + 2p^2 + \sum \gamma_i^2 &= \dim \operatorname{Hom}(F(I(Y)), Y) = 9k^2 + 6 \\ \Rightarrow \sum \gamma_i^2 &= 6 + 5k^2 - 2(r^2 + p^2). \end{aligned} \quad \square$$

**4.2. Twists.** We now compute the twists  $\theta_X : X \rightarrow X$  of the simple objects in  $\mathcal{Z}(\mathcal{C})$ .

**Proposition 4.5.** *The twists satisfy  $\theta_A = \theta_B = \theta_C = 1$ .*

*Proof.* Recall the dimensions of the simple objects  $A, B$ , and  $C$  (see Proposition 4.3). By Theorem 2.5 of [9],

$$6 + 3k\delta = \dim(\mathcal{C}) = \operatorname{Tr}(\theta_{I(1)}) = 1 + (1 + k\delta)\theta_A + (2 + k\delta)\theta_B + (2 + k\delta)\theta_C$$

so we must have  $\theta_A = \theta_B = \theta_C = 1$ .  $\square$

Recall  $\delta = \frac{3k + \sqrt{9k^2 + 12}}{2}$ .

**Lemma 4.6.** *If  $c$  is the squarefree part of  $9k^2 + 12$ , so that  $\delta \in \mathbb{Q}(\sqrt{c})$ , then  $3 \mid c$  and  $(c, 10) = 1$ .*

*Proof.* First,  $9k^2 + 12 = 3(3k^2 + 4)$ , so  $3 \mid 9k^2 + 12$ , giving  $3 \mid c$ . Next, since squares are never  $3 \pmod{5}$ , we have  $5 \nmid 9k^2 + 12 = (3k)^2 + 12$ . Finally, we have  $9k^2 + 12 \equiv 5, 12, 13, 16, 21, 28, 29 \pmod{32}$ , so  $9k^2 + 12$  is always divisible by an even power of 2, and hence  $2 \nmid c$ .  $\square$

Let  $\omega$  be a root of the polynomial  $x^2 + x + 1$ .

**Proposition 4.7.** *The twists satisfy  $\theta_D = \omega$  and  $\theta_E = \theta_G = \theta_H = \theta_J = \omega^2$ .*

*Proof.* By [8], we have

$$\zeta \dim(\mathcal{C}) = \operatorname{Tr}(\theta_{I(X)}^3) = (2 + k\delta) + (2 + \alpha\delta)\theta_D^3 + (1 + r\delta)\theta_E^3 + (1 + p\delta)\theta_G^3.$$

for some root of unity  $\zeta$ . Taking the absolute value of both sides implies  $\theta_D^3 = \theta_E^3 = \theta_G^3 = 1$ . Also, Theorem 2.5 of [9] says that

$$0 = \operatorname{Tr}(\theta_{I(X)}) = (2 + k\delta) + (2 + \alpha\delta)\theta_D + (1 + r\delta)\theta_E + (1 + p\delta)\theta_G,$$

and since  $\delta \notin \mathbb{Q}(\omega)$  this implies

$$0 = 2 + 2\theta_D + \theta_E + \theta_G \quad \text{and} \quad 0 = k + \alpha\theta_D + r\theta_E + p\theta_G.$$

Since  $\theta_D \neq 1$  (otherwise the above equation would be strictly greater than 0), we have  $\theta_D = \omega$  which implies  $\theta_E = \theta_G = \omega^2$ .  $\square$

**Corollary 4.8.** *We have  $\alpha = k$  and  $r + p = k$ .*

*Proof.* We have  $0 = k + \alpha\omega + r\omega^2 + p\omega^2$ . Setting the imaginary part equal to 0 implies  $\alpha = r + p$ . Then, Proposition 4.3 gives  $2k = \alpha + r + p = 2\alpha$ , so we have  $\alpha = k$  and  $r + p = k$ .  $\square$

**4.3. Categorifications of  $K_1(e)$ .** Recall the dimensions of  $A, B, C, D, E, G, H, J \in \mathcal{Z}(\mathcal{C})$  from Proposition 4.3, and the decomposition of  $I(Y)$  from Proposition 4.4. Let  $\theta_i = \theta_{L_i}$ . We will take the trace of  $\theta_{I(Y)}$  and  $\theta_{I(Y)}$  and use the results in [8] to arrive at expressions for the sums of the twists  $\sum \gamma_i \theta_i$  and the sum of their squares  $\sum \gamma_i^2 \theta_i^2$  in terms of the parameter  $k$ . By Theorem 2.5 of [9], we have

$$\begin{aligned} 0 &= \text{Tr}(\theta_{I(Y)}) = k(1 + k\delta) + k(2 + k\delta) + k(2 + k\delta) + k(2 + k\delta)\omega \\ &\quad + 2r(1 + r\delta)\omega^2 + 2p(1 + p\delta)\omega^2 + \sum \gamma_i^2 \theta_i \delta \\ \Rightarrow \quad \sum \gamma_i^2 \theta_i \delta &= -k(1 + k\delta) - k(2 + k\delta) - k(2 + k\delta) - k(2 + k\delta)\omega \\ &\quad - 2r(1 + r\delta)\omega^2 - 2p(1 + p\delta)\omega^2 \\ \sum \gamma_i^2 \theta_i &= \frac{-k}{2}\sqrt{9k^2 + 12} - 2rp \pm \frac{\sqrt{3}i}{2}(k^2 - 4rp). \end{aligned}$$

Next, [8] says that if a simple object  $Y$  is self-dual  $\text{Tr}(\theta_{I(Y)}^2) = \pm \dim(\mathcal{C})$ . We apply this result to  $Y$ :

$$\begin{aligned} \sum \gamma_i^2 \theta_i^2 &= \frac{-k}{2}\sqrt{9k^2 + 12} - 2rp \mp \frac{\sqrt{3}i}{2}(k^2 - 4rp) \pm \frac{\dim(\mathcal{C})}{d} \\ &= \frac{-k}{2}\sqrt{9k^2 + 12} - 2rp \mp \frac{\sqrt{3}i}{2}(k^2 - 4rp) \pm \sqrt{9k^2 + 12}. \end{aligned}$$

We now have expressions for a sum of roots of unity and the sum of their squares equal to some quadratic irrationalities in the same field. We will use the following result, which is proved in section 6, in the proof of Theorem 4.11. In the statement,  $\varphi$  is the Euler-phi function.

**Proposition 4.9.** *Let  $c = \prod_{i=1}^t p_i$  be an odd integer divisible by 3 where the  $p_i$  are distinct primes, and let  $a, b, d \in \mathbb{Z}_{\geq 0}$ . If there are  $N$  roots of unity  $\theta_i$  such that  $\sum \theta_i = -a - b\sqrt{c}$  and  $\sum \theta_i^2 = -a - d\sqrt{c}$ , then  $N \geq P(a, b, c, d)$ , where*

$$P(a, b, c, d) = \begin{cases} b\varphi(c) + d\varphi(c) + b + 2a & \text{if } c \equiv 3 \pmod{4} \text{ and } t \text{ is odd} \\ b\varphi(c) - 2b + 2a & \text{otherwise.} \end{cases}$$

We will also need the following lemma.

**Lemma 4.10.** *Let  $c = 3x \geq 33$  be an odd squarefree integer. Then  $\frac{\varphi(c)}{\sqrt{c}} \geq \frac{\varphi(33)}{\sqrt{33}}$ . Similarly, if  $c = 3x \geq 21$ , then  $\frac{\varphi(c)}{\sqrt{c}} \geq \frac{\varphi(21)}{\sqrt{21}}$ .*

*Proof.* Since  $\frac{\varphi(c)}{\sqrt{c}} = \frac{\varphi(3)}{\sqrt{3}} \cdot \frac{\varphi(x)}{\sqrt{x}}$ , it is sufficient to show that  $\frac{\varphi(x)}{\sqrt{x}} \geq \frac{\varphi(11)}{\sqrt{11}}$ . If  $x$  is prime, then  $\frac{\varphi(x)}{\sqrt{x}} = \frac{x-1}{\sqrt{x}} \geq \frac{11-1}{\sqrt{11}} = \frac{\varphi(11)}{\sqrt{11}}$ . Otherwise,  $x$  is divisible by at least two primes. Since 2 and 3 do not divide  $x$ , we have  $\frac{\varphi(x)}{\sqrt{x}} \geq \frac{\varphi(5)\varphi(7)}{\sqrt{5 \cdot 7}} \geq \frac{\varphi(11)}{\sqrt{11}}$ . Replacing 11 with 7, the argument with 21 becomes identical.  $\square$

**Theorem 4.11.** *Assume the based ring  $K_1(e)$  is categorifiable. Then  $e = 0, 2, 3, 6$ .*

*Proof.* Consider the following sum of roots of unity and the sum of their squares:

$$(13) \quad \sum \gamma_i^2 \theta_i + \sum \gamma_i^2 \bar{\theta}_i = -k\sqrt{9k^2 + 12} - 4rp$$

$$(14) \quad \sum \gamma_i^2 \theta_i^2 + \sum \gamma_i^2 \bar{\theta}_i^2 = (-k \pm 2)\sqrt{9k^2 + 12} - 4rp$$

By Proposition 4.4, (13) and (14) contain at most  $2 \cdot \sum \gamma_i^2 = 12 + 6k^2 + 8rp$  roots of unity. Let  $c$  be the squarefree part of  $9k^2 + 12$ , and let  $a = 4rp$ ,  $b = k\sqrt{\frac{9k^2+12}{c}}$ , and  $d = (k \pm 2)\sqrt{\frac{9k^2+12}{c}}$ . If  $\mathbf{c} = \mathbf{3}$ , then Proposition 4.9 gives

$$\begin{aligned} 12 + 6k^2 + 8rp &\geq P(a, b, c, d) \geq k\sqrt{3k^2+4} \cdot 2 + (k-2)\sqrt{3k^2+4} \cdot 2 + k\sqrt{3k^2+4} + 8rp \\ \Rightarrow 12 + 6k^2 &\geq (5k-4)\sqrt{3k^2+4}. \end{aligned}$$

This fails for  $k > 3$ . When  $k = 3$ , we have  $c = 93$ , so  $k \leq 2$ .

When  $\mathbf{c} \neq \mathbf{3}$ , Proposition 4.9 gives

$$\begin{aligned} 12 + 6k^2 + 8rp &\geq P(a, b, c, d) \geq b\varphi(c) - 2b + 2a \\ &\geq k\sqrt{\frac{9k^2+12}{c}}\varphi(c) - 2k\sqrt{\frac{9k^2+12}{c}} + 8rp \\ 12 + 6k^2 &\geq \frac{\varphi(c)}{\sqrt{c}}k\sqrt{9k^2+12} - 2k\sqrt{\frac{9k^2+12}{c}}. \end{aligned}$$

If  $\mathbf{c} = \mathbf{21}$ , the above equation implies  $k \leq 3$ ; when  $k = 3$  we have  $c = 93$ , so  $k \leq 2$ . When  $\mathbf{c} \geq \mathbf{33}$ , using Lemma 4.10,

$$12 + 6k^2 \geq \frac{\varphi(33)}{\sqrt{33}}k\sqrt{9k^2+12} - 2k\sqrt{\frac{9k^2+12}{33}} \Rightarrow k \leq 2.$$

Thus we have shown that  $k \leq 2$ . This implies  $e = 0, 3, 6$ . However, recall that we have assumed  $e \neq 2$ . Hence, if  $K_1(e)$  admits categorification then  $e = 0, 2, 3, 6$ .  $\square$

## 5. CATEGORIFICATIONS OF $K_2(c)$

We follow a similar technique as in the previous section. Throughout this section, we assume that  $\mathcal{C}$  is a fusion category with  $K(\mathcal{C}) \simeq K_2(c)$  and arrive at a contradiction when  $c > 2$ .  $K_2(0)$  is the based ring (5) of Theorem 1.1, and when  $c = 1, 2$  we get (6). Recall that the multiplication in  $K_2(c)$  is given by

$$\begin{array}{lll} X^2 = cX + Y + cZ & Y^2 = \mathbf{1} & Z^2 = cX + Y + cZ \\ XY = YX = Z & YZ = ZY = X & XZ = ZX = \mathbf{1} + cX + cZ \end{array}$$

**5.1. Induction and Forgetful Functors.** As before, we describe the simple objects in  $\mathcal{Z}(\mathcal{C})$ . Propositions 5.2 and 5.3 give the dimensions of simple objects and their images under the forgetful functor  $F$ . Let  $d = c + \sqrt{c^2 + 1}$ . Note that  $d$  is irrational for  $c > 0$ . Since  $K_2(0)$  is the Grothendieck ring of the category of representations of  $\mathbb{Z}/4\mathbb{Z}$ , and hence already known to admit categorification, we will assume that  $d$  is irrational.

**Proposition 5.1.** *The dimensions of simple objects in  $\mathcal{C}$  are  $\dim(X) = \dim(Z) = d$  and  $\dim(Y) = \dim(\mathbf{1}) = 1$ , whence  $\dim(\mathcal{C}) = 4 + 4cd$ .*

*Proof.* The matrix for left multiplication by  $X$  is

$$M_X = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & c & 0 & c \\ 0 & 1 & 0 & 0 \\ 0 & c & 1 & c \end{pmatrix}.$$

The characteristic polynomial of  $M_X$  is  $x^4 - 2cx^3 - 2cx - 1 = (x^2 + 1)(x^2 - 2cx - 1)$ , so  $\dim(X) = \frac{2c + \sqrt{4c^2 + 4}}{2} = c + \sqrt{c^2 + 1}$ . We know  $\dim(X) = \dim(Z)$  because  $X^* = Z$ . The matrix for left multiplication by  $Y$  is

$$M_Y = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

which has characteristic polynomial  $(x + 1)^2(x - 1)^2$ , so  $\dim(Y) = \dim(\mathbf{1}) = 1$ . We calculate  $\dim(\mathcal{C}) = \dim(\mathbf{1})^2 + \dim(X)^2 + \dim(Y)^2 + \dim(Z)^2 = 2 + 2d^2 = 4 + 4cd$ .  $\square$

**Proposition 5.2.** *There exist non-isomorphic simple objects  $A, B, C, D, E, G, H$  in  $\mathcal{Z}(\mathcal{C})$  for which  $I(\mathbf{1}) = \mathbf{1} \oplus A \oplus B \oplus C$  and  $I(Y) = D \oplus E \oplus G \oplus H$  and*

$$\begin{aligned} F(A) &= \mathbf{1} \oplus cX \oplus cZ & \dim(A) &= 1 + 2cd \\ F(B) &= \mathbf{1} \oplus gX \oplus hZ & \dim(B) &= 1 + cd \\ F(C) &= \mathbf{1} \oplus hX \oplus gZ & \dim(C) &= 1 + cd \\ F(D) &= jX \oplus Y \oplus kZ & \dim(D) &= 1 + (j + k)d \\ F(E) &= lX \oplus Y \oplus mZ & \dim(E) &= 1 + (l + m)d \\ F(G) &= nX \oplus Y \oplus pZ & \dim(G) &= 1 + (n + p)d \\ F(H) &= qX \oplus Y \oplus rZ & \dim(H) &= 1 + (q + r)d \end{aligned}$$

where  $g + h = c$  and  $j + l + n + q = k + m + p + r = 2c$

*Proof.* Two of the formal codegrees of  $K_1(c)$  are  $f_1 = f_2 = 4$ . (see Remark 3.5). By Theorem 2.13 of [9],  $I(\mathbf{1}) \in \mathcal{Z}(\mathcal{C})$  decomposes into the sum of 4 simple objects  $I(\mathbf{1}) = \mathbf{1} \oplus A \oplus B \oplus C$ ; we can assume that  $\dim(B) = \dim(C) = \frac{\dim(\mathcal{C})}{4} = 1 + cd$  whence  $\dim(A) = \frac{\dim(\mathcal{C})}{2} - 1 = 1 + 2cd$ . By Proposition 5.4 of [4],

$$\begin{aligned} F(I(\mathbf{1})) &= \bigoplus_{X \in \mathcal{O}(\mathcal{C})} X \otimes \mathbf{1} \otimes X^* \\ &= \mathbf{1} \oplus (\mathbf{1} \oplus cX \oplus cZ) \oplus \mathbf{1} \oplus (\mathbf{1} \oplus cX \oplus cZ) \\ &= 4 \cdot \mathbf{1} \oplus 2cX \oplus 2cZ \end{aligned}$$

and  $1 + \dim(A) + \dim(B) + \dim(C) = 4 + 4cd$ . Let  $F(A) = \mathbf{1} \oplus aX \oplus bZ$ , whence  $1 + d(a + b) = \dim(A) = 1 + 2cd$  implies  $a + b = 2c$ . Since this decomposition into simple objects is unique and  $I(\mathbf{1})$  is self-dual and the dimension of  $A$  is unique,  $A$  must be self-dual. Hence,  $a = b = c$ .

Now let  $F(B) = \mathbf{1} \oplus gX \oplus hZ$ , whence  $1 + (g + h)d = \dim(B) = 1 + cd$  implies  $g + h = c$ . By duality,  $F(C) = \mathbf{1} \oplus hX \oplus gZ$ . (In the case that  $B$  and  $C$  are self-dual, we have  $g = h$  so this is true in general).

Since  $\dim \operatorname{Hom}(I(\mathbf{1}), I(Y)) = \dim \operatorname{Hom}(F(I(\mathbf{1})), Y) = 0$ , the simple objects in the decomposition of  $I(Y)$  are distinct from  $A, B, C$ . By Proposition 5.4 of [4],

$$\begin{aligned} F(I(Y)) &= \bigoplus_{X \in \mathcal{O}(\mathcal{C})} X \otimes Y \otimes X^* \\ &= Y \oplus (cX \oplus Y \oplus cZ) \oplus Y \oplus (cX \oplus Y \oplus cZ) \\ &= 2cX \oplus 4Y \oplus 2cZ \end{aligned}$$

Hence,  $\dim \operatorname{Hom}(I(Y), I(Y)) = \dim \operatorname{Hom}(F(I(Y)), Y) = 4$ , so either  $I(Y) = 2D$  for some simple object  $D$  or  $I(Y) = D \oplus E \oplus G \oplus H$  for distinct simple objects  $D, E, G, H$ . First assume that  $I(Y) = 2D$ . Then,  $F(D) = cX \oplus 2Y \oplus cZ$ , whence  $\dim(D) = 2 + 2cd$ . Let  $\theta_D$  be the balance isomorphism. Now we have

$$0 = \operatorname{Tr} \theta_{I(Y)} = 2 \dim(D) \theta_D = 2(2 + 2cd) \theta_D$$

which implies  $\theta_D = 0$ , a contradiction. Hence  $I(Y) = D \oplus E \oplus G \oplus H$ .  $\square$

**Proposition 5.3.** *There exist simple objects  $L_i$  distinct from  $A, B, C, D, E, G, H$  in  $\mathcal{Z}(\mathcal{C})$  such that*

- (1)  $F(L_i) = \gamma_i X + \gamma_i^* Z$
- (2)  $I(X) = cA \oplus gB \oplus hC \oplus jD \oplus lE \oplus nG \oplus qH \oplus \sum \gamma_i L_i$
- (3)  $\sum \gamma_i(\gamma_i + \gamma_i^*) \leq 4 + 3c^2$

*Proof.* Let  $L_i = \varphi_i \cdot \mathbf{1} \oplus \gamma_i X \oplus \psi_i Y \oplus \gamma_i^* Z$  such that (1) is satisfied. (We can assume  $\gamma_i \neq 0$  because  $\dim \operatorname{Hom}(L_i, I(X)) = \dim \operatorname{Hom}(F(L_i), X) = \gamma_i$ . That is, if  $\gamma_i = 0$  then  $L_i$  does not appear in the decomposition of  $I(X)$ .) Then we compute

$$\begin{aligned} F(I(X)) &= cF(A) \oplus gF(B) \oplus hF(C) \oplus jF(D) \oplus lF(E) \oplus nF(G) \oplus qF(H) \oplus \sum \gamma_i F(L_i) \\ &= c(\mathbf{1} \oplus cX \oplus cZ) \oplus g(\mathbf{1} \oplus gX \oplus hZ) \oplus h(\mathbf{1} \oplus hX \oplus gZ) \oplus j(jX \oplus Y \oplus kZ) \\ &\quad \oplus l(lX \oplus Y \oplus mZ) \oplus n(nX \oplus Y \oplus pZ) \oplus q(qX \oplus Y \oplus rZ) \\ &\quad \oplus \sum \gamma_i(\varphi_i \cdot \mathbf{1} \oplus \gamma_i X \oplus \psi_i Y \oplus \gamma_i^* Z) \\ &= (c + g + h + \sum \gamma_i \varphi_i) \cdot \mathbf{1} \oplus (c^2 + g^2 + h^2 + j^2 + l^2 + n^2 + q^2 + \sum \gamma_i^2) X \\ &\quad \oplus (j + l + n + q + \sum \gamma_i \psi_i) Y \oplus (c^2 + 2gh + jk + lm + np + qr + \sum \gamma_i \gamma_i^*) Z \end{aligned}$$

Using Theorem 5.4 of [4], we compute

$$F(I(X)) = \bigoplus_{Y \in \mathcal{O}(\mathcal{C})} Y \otimes X \otimes Y^* = 2c \cdot \mathbf{1} + (4 + 4c^2)X + 2cY + 4c^2Z.$$

Hence,  $c + g + h + \sum \gamma_i \varphi_i = 2c$  implies  $\varphi_i = 0$  for all  $i$ . Also  $j + l + n + q + \sum \gamma_i \psi_i = 2c$  implies  $\psi_i = 0$  for all  $i$ .

We are left with the following two equations:

$$(15) \quad c^2 + g^2 + h^2 + (j^2 + l^2 + n^2 + q^2) + \sum \gamma_i^2 = 4 + 4c^2$$

$$(16) \quad c^2 + 2gh + jk + lm + np + qr + \sum \gamma_i \gamma_i^* = 4c^2$$

Because of duality constraints, the set  $\{j, l, n, q\}$  is a permutation of the set  $\{k, m, p, r\}$  so, (15) implies

$$(17) \quad c^2 + g^2 + h^2 + (k^2 + m^2 + p^2 + r^2) + \sum \gamma_i^2 = 4 + 4c^2.$$

We add (15) with (17) and twice (16) to get

$$4c^2 + 2(g + h)^2 + (j + k)^2 + (l + m)^2 + (n + p)^2 + (q + r)^2 + 2 \cdot \sum \gamma_i^2 + 2 \cdot \sum \gamma_i \gamma_i^* = 8 + 16c^2$$

whence,

$$\begin{aligned}
2 \cdot \sum \gamma_i(\gamma_i + \gamma_i^*) &= 8 + 10c^2 - ((j+k)^2 + (l+m)^2 + (n+p)^2 + (q+r)^2) \\
&\leq 8 + 10c^2 - \frac{1}{4}(j+k+l+m+n+p+q+r)^2 \\
&= 8 + 10c^2 - 4c^2 \\
\Rightarrow \sum \gamma_i(\gamma_i + \gamma_i^*) &\leq 4 + 3c^2 \quad \square
\end{aligned}$$

**5.2. Twists.** Using the same methods as in section 4, we calculate the twists for some of the simple objects  $\mathcal{Z}(\mathcal{C})$ .

**Proposition 5.4.** *The twists  $\theta_A = \theta_B = \theta_C = 1$*

*Proof.* By Theorem 2.5 of [9],

$$\begin{aligned}
4 + 4cd &= \dim(\mathcal{C}) = \text{Tr}(\theta_{I(1)}) \\
&= 1 + \dim(A)\theta_A + \dim(B)\theta_B + \dim(C)\theta_C \\
&= 1 + (1 + 2cd)\theta_A + (1 + cd)\theta_B + (1 + cd)\theta_C \quad \square
\end{aligned}$$

Let  $\theta = \theta_D$ .

**Proposition 5.5.** *Without loss of generality, the balance isomorphisms  $\theta_D, \theta_E, \theta_G, \theta_H$  satisfy one of the following*

- (1)  $\theta = \theta_D = \theta_E = -\theta_G = -\theta_H = 1$
- (2)  $\theta = \theta_D = \theta_E = -\theta_G = -\theta_H = i$

*Proof.* By Theorem 2.7 of [9],

$$\begin{aligned}
\pm(4 + 4cd) &= \pm \dim(\mathcal{C}) = \text{Tr}(\theta_{I(Y)}^2) \\
&= \dim(D)\theta_D^2 + \dim(E)\theta_E^2 + \dim(G)\theta_G^2 + \dim(H)\theta_H^2 \\
&= (1 + (j+k)d)\theta_D^2 + (1 + (l+m)d)\theta_E^2 + (1 + (n+p)d)\theta_G^2 + (1 + (q+r)d)\theta_H^2
\end{aligned}$$

Then, since  $j+k+l+m+n+p+q+r = 4c$  we have  $\theta_D^2 = \theta_E^2 = \theta_G^2 = \theta_H^2 = \pm 1$ .

Next, Theorem 2.5 of [9] gives

$$(18) \quad 0 = \text{Tr}(\theta_{I(Y)}) = (1 + (j+k)d)\theta_D + (1 + (l+m)d)\theta_E + (1 + (n+p)d)\theta_G + (1 + (q+r)d)\theta_H.$$

Since the twists are fourth roots of unity and  $d$  is real and irrational, we have  $\theta_D + \theta_E + \theta_G + \theta_H = 0$ , which implies, without loss of generality,  $\theta_D = \theta_E = -\theta_G = -\theta_H$ .  $\square$

**5.3. Categorifications of  $K_2(c)$ .** Let  $\theta_i = \theta_{L_i}$ . Using the results in [8] and calculating the traces of  $\theta_{I(X)}$  and  $\theta_{I(X)}^2$ , we arrive at expressions for linear combinations of the  $\theta_i$  and  $\theta_i^2$ . Using Theorem 2.5 of [9], we compute

$$\begin{aligned}
0 &= \text{Tr}(\theta_{I(X)}) \\
&= c \dim(A)\theta_A + g \dim(B)\theta_B + h \dim(C)\theta_C + j \dim(D)\theta_D + l \dim(E)\theta_E \\
&\quad + n \dim(G)\theta_G + q \dim(H)\theta_H + \sum \gamma_i \dim(L_i)\theta_i \\
&= c(1 + 2cd) + g(1 + cd) + h(1 + cd) + j(1 + (j + k)d)\theta + l(1 + (l + m)d)\theta \\
&\quad - n(1 + (n + p)d)\theta - q(1 + (q + r)d)\theta + \sum \gamma_i(\gamma_i + \gamma_i^*)d\theta_i \\
&= 2c + 3c^2d + \theta(j + l - n - q) + \theta d(j^2 + jk + l^2 + lm - n^2 - np - q^2 - qr) \\
&\quad + \sum \gamma_i(\gamma_i + \gamma_i^*)d\theta_i,
\end{aligned}$$

whence,

$$(19) \quad \sum \gamma_i(\gamma_i + \gamma_i^*)\theta_i = -\frac{2c}{d} - 3c^2 - \frac{\theta}{d}(j + l - n - q) - \theta(j^2 + jk + l^2 + lm - n^2 - np - q^2 - qr).$$

Also by [8],

$$\begin{aligned}
0 &= \text{Tr}(\theta_{I(X)}^2) \\
&= c \dim(A)\theta_A^2 + g \dim(B)\theta_B^2 + h \dim(C)\theta_C^2 + j \dim(D)\theta_D^2 + l \dim(E)\theta_E^2 + n \dim(G)\theta_G^2 \\
&\quad + q \dim(H)\theta_H^2 + \sum \gamma_i \dim(L_i)\theta_i^2 \\
&= 2c + 3c^2d + \theta^2(j + l + n + q) + \theta^2 d(j^2 + jk + l^2 + lm + n^2 + np + q^2 + qr) \\
&\quad + \sum \gamma_i(\gamma_i + \gamma_i^*)d\theta_i^2 \\
&= 2c + 3c^2d + 2c\theta^2 + \theta^2 d(j^2 + jk + l^2 + lm + n^2 + np + q^2 + qr) + \sum \gamma_i(\gamma_i + \gamma_i^*)d\theta_i^2,
\end{aligned}$$

whence

$$(20) \quad \sum \gamma_i(\gamma_i + \gamma_i^*)\theta_i^2 = -\frac{2c}{d} - 3c^2 - \frac{2c}{d}\theta^2 - \theta^2(j^2 + jk + l^2 + lm + n^2 + np + q^2 + qr).$$

Equations 19 and 20 show that a sum of a limited number of roots of unity and the sum of their squares are equal to some quadratic irrationalities. We will be able to get a contradiction when  $c > 2$  using the following results from section 6:

**Proposition 5.6.** *For integers  $a, b$ , it takes at least  $|a| + 2|b|$  roots of unity to write  $a + b\sqrt{2}$  as a sum of roots of unity.*

**Theorem 5.7.** *For  $d$  square-free it requires at least  $|b|\varphi(2d)$  roots of unity to write  $a + b\sqrt{d}$  as a sum of roots of unity.*

**Theorem 5.8.** *If the based ring  $K_2(c)$  is categorifiable, then  $c \leq 2$ .*

*Proof.* Assume there exists a category  $\mathcal{C}$  such that  $K(\mathcal{C}) = K_2(c)$ . We now consider the two cases outlined in Proposition 5.5.

**Case 1:  $\theta = 1$ .** Then, (20) becomes

$$\begin{aligned}
\sum \gamma_i(\gamma_i + \gamma_i^*)\theta_i^2 &= -\frac{4c}{d} - 3c^2 - (j^2 + jk + l^2 + lm + n^2 + np + q^2 + qr) \\
&= -4c\sqrt{c^2 + 1} + 4c^2 - 3c^2 - (j^2 + jk + l^2 + lm + n^2 + np + q^2 + qr)
\end{aligned}$$

The right hand side of the above equation requires at least

$$4c\sqrt{\frac{c^2+1}{2}} \cdot 2 \geq \frac{8}{\sqrt{2}}c^2$$

roots of unity to write, while the left hand side contains at most  $\sum \gamma_i(\gamma_i + \gamma_i^*)$  roots of unity. Hence,

$$4 + 3c^2 \geq \sum \gamma_i(\gamma_i + \gamma_i^*) \geq \frac{8}{\sqrt{2}}c^2,$$

which implies  $c \leq 1$ . Note that if  $c = 1$ , then we have  $4c\sqrt{\frac{c^2+1}{2}} \cdot 2 = 8 > 7 = 4 + 3c^2$ , so in fact,  $c < 1$ .

**Case 2:  $\theta = i$ .** Then, (19) becomes

$$\begin{aligned} \sum \gamma_i(\gamma_i + \gamma_i^*)\theta_i &= -\frac{2c}{d} - 3c^2 - \frac{i}{d}(j + l - n - q) - i(j^2 + jk + l^2 + lm - n^2 - np - q^2 - qr) \\ &= -2c\sqrt{c^2+1} - c^2 - \frac{i}{d}(j + l - n - q) - i(j^2 + jk + l^2 + lm - n^2 - np - q^2 - qr), \end{aligned}$$

whence

$$(21) \quad \sum \gamma_i(\gamma_i + \gamma_i^*)\theta_i + \sum \gamma_i(\gamma_i + \gamma_i^*)\overline{\theta_i} = -4c\sqrt{c^2+1} - 2c^2$$

If  $c^2 + 1$  is 2 times a square, then Proposition 5.6 implies that right hand side of (21) requires at least

$$4c\sqrt{\frac{c^2+1}{2}} \cdot 2 + 2c^2 \geq \left(\frac{8}{\sqrt{2}} + 2\right)c^2$$

roots of unity to write, while the left hand side contains at most  $2 \cdot \sum \gamma_i(\gamma_i + \gamma_i^*)$  roots of unity. Hence,

$$8 + 6c^2 \geq 2 \cdot \sum \gamma_i(\gamma_i + \gamma_i^*) \geq \left(\frac{8}{\sqrt{2}} + 2\right)c^2,$$

which implies  $c \leq 2$ .

If  $c^2 + 1$  is not 2 times a square, then Theorem 5.7 implies that the right hand side of (21) requires at least

$$4c\sqrt{\frac{c^2+1}{5}} \cdot 4 \geq \frac{16}{\sqrt{5}}c^2$$

roots of unity to write, so

$$8 + 6c^2 \geq 2 \cdot \sum \gamma_i(\gamma_i + \gamma_i^*) \geq \frac{16}{\sqrt{5}}c^2,$$

which implies  $c \leq 2$ . □

## 6. SUMS OF ROOTS OF UNITY

In the proofs of Theorems 4.11 and 5.8, we needed tight bounds on the number of roots of unity required to write certain quadratic irrationalities. To develop these bounds, we will make use the following observation: suppose we have  $N$  roots of unity  $\theta_i$  in  $\mathbb{Q}(\zeta_x)$  such that  $\sum \theta_i = a + b\sqrt{c}$  for integers  $a, b, c$ . Then summing over all Galois conjugates (by  $\text{Gal}(\mathbb{Q}(\zeta_x)/\mathbb{Q}(\sqrt{c}))$ ) of this equation gives a collection of  $MN$  roots of unity, where  $M = |\text{Gal}(\mathbb{Q}(\zeta_x)/\mathbb{Q}(\sqrt{c}))|$ , whose sum is  $M(a + b\sqrt{c})$  and whose multiplicities are Galois-invariant. Hence, if it requires at least  $MA$  roots of unity to write  $M(a + b\sqrt{c})$  such that the multiplicities are Galois-invariant, it



requires at least  $A$  roots of unity to write  $a + b\sqrt{c}$ . This reduces the problem to a question about sums of Galois orbits.

**Lemma 6.1.** *Let  $a, b, c$  be integers with  $c = 2^\alpha \prod p_i$  the product of distinct primes. Define  $\epsilon = 0$  if  $c \equiv 1 \pmod{4}$  and  $\epsilon = 1$  if  $c \equiv 2, 3 \pmod{4}$ . Assume there exist  $N$  roots of unity  $\theta_i$  in some cyclotomic field  $\mathbb{Q}(\zeta_x)$  such that*

$$(22) \quad \sum \theta_i = a + b\sqrt{c}$$

*Then, for some positive integer  $M$ , there exists a collection of less than or equal to  $MN$  roots of unity  $\theta'_i$  with*

$$(23) \quad \sum \theta'_i = M(a + b\sqrt{c})$$

*such that the multiplicity of  $\theta'_i$  is  $\text{Gal}(\mathbb{Q}(\zeta_x)/\mathbb{Q}(\sqrt{c}))$ -invariant, and the  $\theta'_i$  are all  $(2^{\epsilon+1}c)^{\text{th}}$  roots of unity.*

*Proof.* Define  $n = 2^{2\epsilon}c$ . Let  $M = |\text{Gal}(\mathbb{Q}(\zeta_x)/\mathbb{Q}(\sqrt{c}))|$ . Summing all Galois conjugates of (22) by  $\text{Gal}(\mathbb{Q}(\zeta_x)/\mathbb{Q}(\sqrt{c}))$  gives an expression in which the multiplicity of  $\theta'_i$  is Galois-invariant. Consider some Galois orbit  $O$  and suppose that all elements of  $O$  are primitive  $Y^{\text{th}}$  roots of unity where  $Y = 2^\beta \prod p_i^{r_i} \prod q_i^{s_i}$ .

**Case 1:**  $n \nmid Y$  Then  $\sqrt{c} \notin \mathbb{Q}(\zeta_Y)$ , so the orbit contains all primitive  $Y^{\text{th}}$  roots of unity and one of the following three things happens:

- (1)  $\sum_{\zeta \in O} \zeta = 1$ ; we replace  $O$  by 1.
- (2)  $\sum_{\zeta \in O} \zeta = -1$ ; we replace  $O$  by  $-1$ .
- (3)  $\sum_{\zeta \in O} \zeta = 0$ ; we drop this orbit from our sums.

All of these replacements have size less than or equal to  $|O|$  and all contain  $(2^{\epsilon+1}c)^{\text{th}}$  roots of unity.

**Case 2:**  $n \mid Y$  and  $\beta > 1 + \epsilon$  or  $r_l > 1$  for some  $l$ . Define  $k = 2$  if  $\beta > 1 + \epsilon$ , and  $k = p_l$  otherwise. Note that,  $p_j \mid Y/k$  for all  $j$ , and  $2 \mid Y/k$ , so if  $i$  is relatively prime to  $Y$  then  $Y/k + i$  is relatively prime to  $Y$ . Hence, for any primitive  $Y^{\text{th}}$  root of unity  $\zeta_Y^i$ ,

$$\zeta_k \cdot \zeta_Y^i = \zeta_Y^{Y/k+i}$$

is also a primitive  $Y^{\text{th}}$  root of unity. In addition,  $n \mid Y/k$  implies that  $Y/k + i \equiv i \pmod{n}$ , so  $\frac{Y/k+i}{i} \equiv 1 \pmod{n}$ . That is,

$$\zeta_k \cdot \zeta_Y^i = \zeta_Y^{Y/k+i} = (\zeta_Y^i)^{\frac{Y/k+i}{i}}$$

is Galois conjugate to  $\zeta_Y^i$  over  $\mathbb{Q}(\zeta_n) \supseteq \mathbb{Q}(\sqrt{c})$ . Hence,

$$\sum_{\zeta \in O} \zeta = \sum_{\zeta \in O} \zeta_k \cdot \zeta = \zeta_k \sum_{\zeta \in O} \zeta.$$

Since  $k > 1$  this implies  $\sum_{\zeta \in O} \zeta = 0$ . Thus we can drop  $O$  from our sums.

**Case 3:**  $n \mid Y$  and  $\beta \leq 1 + \epsilon$  and  $r_l \leq 1$  for all  $l$ . Let  $u = \prod q_i^{s_i}$  and  $v = 2^\beta \prod p_i^{r_i}$  so that  $Y = uv$  and  $(u, v) = 1$ . By the Chinese Remainder Theorem, any  $Y^{\text{th}}$  root of unity can be written uniquely as a  $u^{\text{th}}$  root of unity times a  $v^{\text{th}}$  root of unity, and  $\text{Gal}(\mathbb{Q}(\zeta_Y)/\mathbb{Q}) = \text{Gal}(\mathbb{Q}(\zeta_u)/\mathbb{Q}) \oplus \text{Gal}(\mathbb{Q}(\zeta_v)/\mathbb{Q})$ . Any element of  $\text{Gal}(\mathbb{Q}(\zeta_u)/\mathbb{Q})$  can be seen as an element of  $\text{Gal}(\mathbb{Q}(\zeta_Y)/\mathbb{Q}(\sqrt{c}))$ . (If  $\sqrt{c} \in \mathbb{Q}(\zeta_Y)$ , then  $n \mid Y$ ; since  $(n, u) = 1$ , it follows that  $n \mid v$  so  $\sqrt{c} \in \mathbb{Q}(\zeta_v)$ .) Thus, there is an orbit  $O'$  of primitive  $v^{\text{th}}$  roots of unity so that  $O = \{\zeta_u \zeta_v : \zeta_u \text{ is a primitive } u^{\text{th}} \text{ root of unity and } \zeta_v \in O'\}$ . Hence,

$$\sum_{\zeta \in O} \zeta = \sum_{\zeta_v \in O'} \zeta_v \cdot \sum_{i, (i, u)=1} \zeta_u$$

If  $u$  is not squarefree then  $\sum_{\zeta \in O} \zeta = 0$  so we can remove  $O$  from our sum. If  $u$  is a squarefree product of an even number of primes,  $\sum_{\zeta \in O} \zeta = \sum_{\zeta_v \in O'} \zeta_v$ , so we can replace  $O$  by  $O'$  (which is an orbit containing  $2^{\epsilon+1}c^{\text{th}}$  roots of unity because  $v \mid 2^{\epsilon+1}c$ ). Lastly, if  $u$  is a squarefree product of an odd number of primes,  $\sum_{\zeta \in O} \zeta = -1 \cdot \sum_{\zeta_v \in O'} \zeta_v$ , so we replace  $O$  by  $-1 \cdot O'$ . This is a collection of  $\text{LCM}(2, v)^{\text{th}}$  roots of unity, and since  $\text{LCM}(2, v) \mid 2^{\epsilon+1}c$ , this leaves us with a Galois-invariant collection of  $2^{\epsilon+1}c^{\text{th}}$  roots of unity.  $\square$

**Theorem 6.2** (Theorem 5.7). *For  $c$  square-free it requires at least  $|b|\varphi(2c)$  roots of unity to write  $a + b\sqrt{c}$  as a sum of roots of unity.*

*Proof.* Assume to the contrary that we could write  $a + b\sqrt{c}$  with less than  $|b|\varphi(2c)$  roots of unity in some cyclotomic field  $\mathbb{Q}(\zeta_x)$ . Let  $n = 2c$  if  $c \equiv 1 \pmod{4}$  and  $n = 4c$  if  $c \equiv 2, 3 \pmod{4}$ . Then by Lemma 6.1, for some  $M$ , we could write  $\sum \theta'_i = M(a + b\sqrt{c})$  with less than  $M|b|\varphi(c)$  roots of unity, where the  $\theta'_i$  are all  $n^{\text{th}}$  roots of unity whose multiplicities are  $\text{Gal}(\mathbb{Q}(\zeta_x)/\mathbb{Q}(\sqrt{c}))$ -invariant. Consider some orbit of primitive  $Y^{\text{th}}$  roots of unity.

**Case 1:**  $\sqrt{c} \notin \mathbb{Q}(\zeta_Y)$  The orbit consists of all primitive  $Y^{\text{th}}$  roots of unity so the orbit sums to 0 or  $\pm 1$ , and the coefficient of  $\sqrt{c}$  in the sum of the orbit is 0.

**Case 2:**  $\sqrt{c} \in \mathbb{Q}(\zeta_Y)$  and  $c \equiv 2, 3 \pmod{4}$  By Lemma 6.1, the only case that remains is  $Y = 4c$ . Here there are two Galois orbits  $O_1$  and  $O_2$  of  $4c^{\text{th}}$  roots of unity. We compute

$$\sum_{\zeta \in O_1} \zeta + \sum_{\zeta \in O_2} \zeta = 0,$$

and when we take the difference, it is the product of Gauss sums (see [13] Section 5.5, Equation 6):

$$\sum_{\zeta \in O_1} \zeta - \sum_{\zeta \in O_2} \zeta = 2\sqrt{c}$$

Hence,

$$\sum_{\zeta \in O_1} \zeta = \sqrt{c} \quad \text{and} \quad \sum_{\zeta \in O_2} \zeta = -\sqrt{c},$$

and

$$|O_1| = |O_2| = \frac{1}{2}\varphi(4c) = \varphi(2c).$$

**Case 3:**  $\sqrt{c} \in \mathbb{Q}(\zeta_Y)$  and  $c \equiv 1 \pmod{4}$  By Lemma 6.1, it remains to consider when  $Y = c, 2c$ . We make a similar calculation as above, taking the top sign when  $c \equiv 5 \pmod{8}$  and the lower sign when  $c \equiv 1 \pmod{8}$ , to produce the table:

orbit	size	sum of orbit
$Y = c$	$\frac{1}{2}\varphi(2c)$	$\frac{1}{2}((-1)^t + \sqrt{c})$
$Y = c$	$\frac{1}{2}\varphi(2c)$	$\frac{1}{2}((-1)^t - \sqrt{c})$
$Y = 2c$	$\frac{1}{2}\varphi(2c)$	$\frac{1}{2}((-1)^{t+1} \pm \sqrt{c})$
$Y = 2c$	$\frac{1}{2}\varphi(2c)$	$\frac{1}{2}((-1)^{t+1} \mp \sqrt{c})$

In all cases, the coefficient of  $\sqrt{c}$  over the size of the orbit has absolute value less than or equal to  $1/\varphi(2c)$ . Hence it requires at least  $M|b|\varphi(2c)$  roots of unity to write  $M(a + b\sqrt{c})$  as the sum of roots of unity whose multiplicities are  $\text{Gal}(\mathbb{Q}(\zeta_x)/\mathbb{Q}(\sqrt{c}))$ -invariant.  $\square$

*Remark 6.3.* In some cases the above bound is sharp. For example, when  $c \equiv 1 \pmod{4}$  and  $|a| \leq |b|$ .

In the case when  $c = 2$  we need an even better bound on the roots of unity needed to represent  $a + b\sqrt{c}$ .

**Proposition 6.4** (Proposition 5.6). *For integers  $a, b$ , it takes at least  $|a| + 2|b|$  roots of unity to write  $a + b\sqrt{2}$  as a sum of roots of unity.*

*Proof.* Assume to the contrary that we could write  $a + b\sqrt{2}$  with less than  $|a| + 2|b|$  roots of unity. Then, Lemma 6.1 says that there exists some  $M$  such that we can write  $M(a + b\sqrt{2})$  as the sum of less than  $M(a + 2b)$  roots of unity which are  $8^{\text{th}}$  roots of unity whose multiplicities are invariant under the action of  $\text{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}(\sqrt{2}))$ . For every  $Y$  with  $Y \mid 8$  there is either one orbit which contains all primitive  $Y^{\text{th}}$  roots of unity or two orbits ( $*$  and  $\dagger$ ) which each contain half of the primitive  $Y^{\text{th}}$  roots of unity. We write down the following table:

orbit	size	sum of orbit
$Y = 1$	1	1
$Y = 2$	1	-1
$Y = 4$	2	0
$Y = 8^*$	2	$\sqrt{2}$
$Y = 8^\dagger$	2	$-\sqrt{2}$

Define the linear function  $f(x + y\sqrt{2}) = x + 2y$ . Note that for all orbits, we have

$$-1 \leq \frac{1}{|O_i|} f\left(\sum_{\zeta \in O_i} \zeta\right)$$

Assume there were orbits  $O_1, \dots, O_n$  such that

$$\sum_i \sum_{\zeta \in O_i} \zeta = M(-a - b\sqrt{2}).$$

Then

$$\begin{aligned} \sum_i |O_i| \cdot (-1) &\leq \sum_i |O_i| \cdot \frac{1}{|O_i|} f\left(\sum_{\zeta \in O_i} \zeta\right) = \sum_i f\left(\sum_{\zeta \in O_i} \zeta\right) = f\left(\sum_i \sum_{\zeta \in O_i} \zeta\right) \\ &= f\left(M(-a - b\sqrt{2})\right) = -Mf(a + b\sqrt{c}) = -M(a + 2b) \\ &\Rightarrow \sum_i |O_i| \geq M(a + 2b). \end{aligned}$$

Hence, the number of roots of unity needed to write  $M(a + b\sqrt{2})$  is greater than  $M(a + 2b)$ . This is a contradiction, so it requires at least  $|a| + 2|b|$  roots of unity to write  $a + b\sqrt{2}$ .  $\square$

When studying  $K_1(e)$ , we had a special case where the sum of the squares of the roots of unity is another given quadratic irrationality in the same field. The following lemma is analgous to lemma 6.1, but keeps track of sums of squares of roots of unity as well.

**Lemma 6.5.** *Let  $c = 2^a \prod p_i$  be the product of distinct primes. Define  $\epsilon = 0$  if  $c \equiv 1 \pmod{4}$  and  $\epsilon = 1$  if  $c \equiv 2, 3 \pmod{4}$ . Let  $L = \text{LCM}(2^{\epsilon+2}c, 3)$ . Let  $\alpha$  and  $\beta$  be algebraic integers in  $\mathbb{Z}(\sqrt{c})$ . Assume there exist  $N$  roots of unity  $\theta_i$  in some cyclotomic field  $\mathbb{Q}(\zeta_x)$  such that*

$$(24) \quad \sum \theta_i = \alpha \quad \text{and} \quad \sum \theta_i^2 = \beta.$$

Then, for some positive integer  $M$ , there exists a collection of less than or equal to  $MN$  roots of unity  $\theta'_i$  with

$$(25) \quad \sum \theta'_i = M\alpha \quad \text{and} \quad \sum (\theta'_i)^2 = M\beta,$$

such that the multiplicity of  $\theta'_i$  is  $\text{Gal}(\mathbb{Q}(\zeta_x)/\mathbb{Q}(\sqrt{c}))$ -invariant, and the  $\theta'_i$  are all  $L^{\text{th}}$  roots of unity.

*Proof.* Define  $n = 2^{2\epsilon}c$ . We argue exactly as in Lemma 6.1, but with the following modifications to keep track of the sums of the squares in each orbit:

**Case 1:  $n \nmid Y$**  One of the following four things happens:

- (1)  $Y$  is odd, so  $\sum_{\zeta \in O} \zeta = \sum_{\zeta \in O} \zeta^2 = \pm 1$  or 0. If we have  $+$  we replace  $O$  by the orbit containing only 1; if we have  $-$  we replace  $O$  by the orbit containing 3<sup>rd</sup> roots of unity; and if we have 0, we drop the orbit from our sums.
- (2)  $2 \parallel Y$  and  $\sum_{\zeta \in O} \zeta = \pm 1$  and  $\sum_{\zeta \in O} \zeta^2 = \mp 1$ . If we have the top sign we replace  $O$  by the orbit of primitive 6<sup>th</sup> roots of unity; if we have the bottom sign we replace  $O$  by the orbit containing  $-1$ .
- (3)  $4 \parallel Y$  and  $\sum_{\zeta \in O} \zeta = 0$  and  $\sum_{\zeta \in O} \zeta^2 = \pm 2$ . If we have the top sign we replace  $O$  by the orbit of primitive 12<sup>th</sup> roots of unity; if we have the bottom sign we replace  $O$  by the orbit of primitive 4<sup>th</sup> roots of unity.
- (4)  $8 \mid Y$  and  $\sum_{\zeta \in O} \zeta = \sum_{\zeta \in O} \zeta^2 = 0$ . We drop this orbit from our sums.

All of these replacement orbits have size less than or equal to  $|O|$  and all contain  $L^{\text{th}}$  roots of unity.

**Case 2:  $n \mid Y$  and  $b > 2 + \epsilon$  or  $r_l > 1$  for some  $l$ .** Define  $k = 4$  if  $b > 2 + \epsilon$ , and  $k = p_l$  otherwise. We argue as before, and note that

$$\sum_{\zeta \in O} \zeta^2 = \sum_{\zeta \in O} \zeta_k^2 \cdot \zeta^2 = \zeta_k^2 \sum_{\zeta \in O} \zeta^2.$$

Since  $k > 2$  this implies  $\sum_{\zeta \in O} \zeta = \sum_{\zeta \in O} \zeta^2 = 0$ . Thus we can drop  $O$  from our sums.

**Case 3:  $n \mid Y$  and  $b \leq 2 + \epsilon$  and  $r_i \leq 1$  for all  $i$ .** Note that since  $u$  is odd, the squares of the primitive  $u^{\text{th}}$  roots of unity are the primitive  $u^{\text{th}}$  roots of unity, so

$$\sum_{\zeta \in O} \zeta = \sum_{\zeta_v \in O'} \zeta_v \cdot \sum_{i, (i,u)=1} \zeta_u \quad \text{and} \quad \sum_{\zeta \in O} \zeta^2 = \sum_{\zeta_v \in O'} \zeta_v^2 \cdot \sum_{i, (i,u)=1} \zeta_u.$$

If  $u$  is not squarefree then  $\sum_{\zeta \in O} \zeta = \sum_{\zeta \in O} \zeta^2 = 0$  so we can remove  $O$  from our sum. If  $u$  is a squarefree product of an even number of primes,  $\sum_{\zeta \in O} \zeta = \sum_{\zeta_v \in O'} \zeta_v$  and  $\sum_{\zeta \in O} \zeta^2 = \sum_{\zeta_v \in O'} \zeta_v^2$ , so we can replace  $O$  by  $O'$  (which is an orbit containing  $L^{\text{th}}$  roots of unity because  $v \mid n$  implies  $v \mid L$ ). Lastly, if  $u$  is a squarefree product of an odd number primes,  $\sum_{\zeta \in O} \zeta = (\omega + \omega^2) \sum_{\zeta_v \in O'} \zeta_v$ , and  $\sum_{\zeta \in O} \zeta^2 = (\omega^2 + \omega^4) \sum_{\zeta_v \in O'} \zeta_v^2$  where  $\omega$  is a primitive cube root of unity. Replacing  $O$  by  $\omega O' + \omega^2 O'$  leaves us with a Galois-invariant collection of  $L^{\text{th}}$  roots of unity.  $\square$

**Definition 6.6.** For nonnegative integers  $a, b, c, d$ , with  $c = \prod_{i=1}^t p_i$  squarefree, we define

$$P(a, b, c, d) = \begin{cases} b\varphi(c) + d\varphi(c) + b + 2a & \text{if } c \equiv 3 \pmod{4} \text{ and } t \text{ is odd} \\ b\varphi(c) - 2b + 2a & \text{otherwise.} \end{cases}$$

**Proposition 6.7** (Proposition 4.9). *Let  $c = \prod_{i=1}^t p_i$  be an odd integer divisible by 3 where the  $p_i$  are distinct primes, and let  $a, b, d \in \mathbb{Z}_{\geq 0}$ . If there are  $N$  roots of unity  $\theta_i$  such that  $\sum \theta_i = -a - b\sqrt{c}$  and  $\sum \theta_i^2 = -a - d\sqrt{c}$ , then  $N \geq P(a, b, c, d)$ .*

*Proof.* Assume to the contrary that we could write  $\sum \theta_i = -a - b\sqrt{c}$  and  $\sum \theta_i^2 = -a - d\sqrt{c}$  with less than  $P(a, b, c, d)$  roots of unity. Let  $n = 2c$  if  $c \equiv 1 \pmod{4}$  and  $n = 4c$  if  $c \equiv 3 \pmod{4}$ . Then by Lemma 6.5, for some  $M$ , we could write

$$(26) \quad \sum \theta'_i = M(-a - b\sqrt{c}) \quad \text{and} \quad \sum \theta_i'^2 = M(-a - d\sqrt{c})$$

with less than  $M \cdot P(a, b, c, d)$  roots of unity, where the  $\theta'_i$  are  $2n^{\text{th}}$  roots of unity whose multiplicities are Galois-invariant. To show we need at least  $M \cdot P(a, b, c, d)$  roots of unity  $\theta_i$  to write (26), take some orbit with primitive  $Y^{\text{th}}$  roots of unity. First we consider the case when  $\sqrt{c} \notin \mathbb{Q}(\zeta_Y)$ , so the orbit consists of all primitive  $Y^{\text{th}}$  roots of unity. Write  $Y = 2^b \prod_{i=1}^k p_i^{r_i}$ . We compute:

type of orbit	size	sum of orbit	sum of squares in orbit
$b \geq 3$ , or $r_i > 1$ for some $i$	$\varphi(Y) \geq 0$	0	0
$b = 0$ , $k$ even, $r_i = 1 \forall i$	$\varphi(Y) \geq 1$	1	1
$b = 0$ , $k$ odd, $r_i = 1 \forall i$	$\varphi(Y) \geq 2$	-1	-1
$b = 1$ , $k$ even, $r_i = 1 \forall i$	$\varphi(Y) \geq 1$	-1	1
$b = 1$ , $k$ odd, $r_i = 1 \forall i$	$\varphi(Y) \geq 2$	1	-1
$b = 2$ , $k$ even, $r_i = 1 \forall i$	$\varphi(Y) \geq 1$	0	-2
$b = 2$ , $k$ odd, $r_i = 1 \forall i$	$\varphi(Y) \geq 4$	0	2

To find the minimum number of roots of unity  $\theta_i$  used to write (26), if we can write one row as the sum of other rows in a way that requires less roots of unity, we can assume we do not use that row. Deleting rows in this way, we arrive at the following:

orbit	size	sum of orbit	sum of squares in orbit
$Y = 1$	1	1	1
$Y = 2$	1	-1	1
$Y = 3$	2	-1	-1
$Y = 6$	2	1	-1
$Y = 4$	2	0	-2

Assume  $c \equiv 3 \pmod{4}$ . The cases that remain are  $Y = 4c, 8c$ . Here there are two Galois orbits  $O_1$  and  $O_2$  of  $Y^{\text{th}}$  roots of unity. We compute  $\sum_{\zeta \in O_1} \zeta + \sum_{\zeta \in O_2} \zeta = 0$  and

$$\sum_{\zeta \in O_1} \zeta^2 + \sum_{\zeta \in O_2} \zeta^2 = \begin{cases} 0 & \text{if } Y = 8c; \\ 2 \cdot (-1)^{t+1} & \text{if } Y = 4c. \end{cases}$$

When we take the differences, this is the product of Gauss sums:

$$\sum_{\zeta \in O_1} \zeta - \sum_{\zeta \in O_2} \zeta = \begin{cases} 0 & \text{if } Y = 8c \\ 2\sqrt{c} & \text{if } Y = 4c \end{cases} \quad \text{and} \quad \sum_{\zeta \in O_1} \zeta^2 - \sum_{\zeta \in O_2} \zeta^2 = \begin{cases} \pm 4\sqrt{c} & \text{if } Y = 8c \\ 0 & \text{if } Y = 4c \end{cases}$$

Solving these systems of equations, we have:

orbit	size	sum of orbit	sum of squares in orbit
$Y = 4c$	$\varphi(c)$	$\sqrt{c}$	$(-1)^{t+1}$
$Y = 4c$	$\varphi(c)$	$-\sqrt{c}$	$(-1)^{t+1}$
$Y = 8c$	$2\varphi(c)$	0	$2\sqrt{c}$
$Y = 8c$	$2\varphi(c)$	0	$-2\sqrt{c}$

When  $t$  is odd, define the linear function  $f(x + y\sqrt{c}, z + w\sqrt{c}) = y\varphi(c) + w\varphi(c) + x + z + y$ . If there were orbits  $O_1, \dots, O_m$  with  $\sum_i \sum_{\zeta \in O_i} \zeta = M(-a - b\sqrt{c})$  and  $\sum_i \sum_{\zeta \in O_i} \zeta^2 = M(-a - d\sqrt{c})$ ,

$$\sum_i |O_i| \cdot \frac{1}{|O_i|} f\left(\sum_{\zeta \in O_i} \zeta, \sum_{\zeta \in O_i} \zeta^2\right) = f\left(\sum_i \sum_{\zeta \in O_i} \zeta, \sum_i \sum_{\zeta \in O_i} \zeta^2\right) = -M(b\varphi(c) + d\varphi(c) + 2a + b).$$

Since  $-1 \leq \frac{1}{|O_i|} f(\sum_{\zeta \in O_i} \zeta, \sum_{\zeta \in O_i} \zeta^2)$  for all  $i$ ,

$$\begin{aligned} \sum_i |O_i| \cdot (-1) &\leq \sum_i |O_i| \cdot \frac{1}{|O_i|} f\left(\sum_{\zeta \in O_i} \zeta, \sum_{\zeta \in O_i} \zeta^2\right) = -M(b\varphi(c) + d\varphi(c) + 2a + b) \\ &\Rightarrow \sum_i |O_i| \geq M(b\varphi(c) + d\varphi(c) + 2a + b). \end{aligned}$$

Next, assume  $c \equiv 1 \pmod{4}$ . It remains to consider  $Y = c, 2c, 4c$ . We make a similar calculation as above, taking the top sign when  $c \equiv 5 \pmod{8}$  and the lower sign when  $c \equiv 1 \pmod{8}$ , to produce the table:

orbit	size	sum of orbit	sum of squares in orbit
$Y = c$	$\frac{1}{2}\varphi(c)$	$\frac{1}{2}((-1)^t + \sqrt{c})$	$\frac{1}{2}((-1)^t \mp \sqrt{c})$
$Y = c$	$\frac{1}{2}\varphi(c)$	$\frac{1}{2}((-1)^t - \sqrt{c})$	$\frac{1}{2}((-1)^t \pm \sqrt{c})$
$Y = 2c$	$\frac{1}{2}\varphi(c)$	$\frac{1}{2}((-1)^{t+1} \pm \sqrt{c})$	$\frac{1}{2}((-1)^t + \sqrt{c})$
$Y = 2c$	$\frac{1}{2}\varphi(c)$	$\frac{1}{2}((-1)^{t+1} \mp \sqrt{c})$	$\frac{1}{2}((-1)^t - \sqrt{c})$
$Y = 4c$	$\varphi(c)$	0	$(-1)^{t+1} + \sqrt{c}$
$Y = 4c$	$\varphi(c)$	0	$(-1)^{t+1} - \sqrt{c}$

Define the function  $f(x + y\sqrt{c}, z + w\sqrt{c}) = y\varphi(c) + x + z - 2y$ . Assume there were orbits  $O_1, \dots, O_n$  such that  $\sum_i \sum_{\zeta \in O_i} \zeta = M(-a - b\sqrt{c})$  and  $\sum_i \sum_{\zeta \in O_i} \zeta^2 = M(-a - d\sqrt{c})$ . In all cases, we find

$$-1 \leq \frac{1}{|O|} f\left(\sum_{\zeta \in O} \zeta, \sum_{\zeta \in O} \zeta^2\right).$$

So by the same argument as above, we have  $\sum_i |O_i| \geq M(b\varphi(c) + 2a - 2b)$ .  $\square$

**Acknowledgements.** I would like to thank Victor Ostrik for suggesting this problem, providing me with useful papers to read, and meeting with me weekly to discuss ideas. I would also like to thank my brother, Eric Larson, for teaching me about the theory of cyclotomic fields (such as some of the methods used in section 6) and proof-reading the paper.

## REFERENCES

- [1] Bojko Bakalov and Alexander Kirillov, Jr. *Lectures on tensor categories and modular functors*, volume 21 of *University Lecture Series*. American Mathematical Society, Providence, RI, 2001.
- [2] Paul Bruillard. Rank 4 premodular categories. [arXiv:1204.4836](#).
- [3] Frank Calegari, Scott Morrison, and Noah Snyder. Cyclotomic integers, fusion categories, and subfactors. *Comm. Math. Phys.*, 303(3):845–896, 2011.
- [4] Pavel Etingof, Dmitri Nikshych, and Viktor Ostrik. On fusion categories. *Ann. of Math. (2)*, 162(2):581–642, 2005.
- [5] Seung-moon Hong and Eric Rowell. On the classification of the grothendieck rings of non-self-dual modular categories. *Journal of Algebra*, 324(5):1000–1015, 2010.

- [6] Zhengwei Liu, Scott Morrison, and David Penneys. 1-supertransitive subfactors with index at most  $6+1/5$ . [arXiv:1310.8566](#).
- [7] G. Lusztig. Leading coefficients of character values of Hecke algebras. In *The Arcata Conference on Representations of Finite Groups (Arcata, Calif., 1986)*, volume 47 of *Proc. Sympos. Pure Math.*, pages 235–262. Amer. Math. Soc., Providence, RI, 1987.
- [8] Siu-Hung Ng and Peter Schauenburg. Frobenius-Schur indicators and exponents of spherical categories. *Adv. Math.*, 211(1):34–71, 2007.
- [9] Victor Ostrik. Pre-modular categories of rank 3. *Mosc. Math. J.*, 8(1):111–118, 184, 2008.
- [10] Victor Ostrik. On formal codegrees of fusion categories. *Math. Res. Lett.*, 16(5):895–901, 2009.
- [11] Viktor Ostrik. Fusion categories of rank 2. *Math. Res. Lett.*, 10(2-3):177–183, 2003.
- [12] Eric Rowell, Richard Strong, and Zhenghan Wang. On classification of modular tensor categories. *Comm. Math. Phys.*, 292(2):343389, 2009.
- [13] Pierre Samuel. *Algebraic theory of numbers*. Translated from the French by Allan J. Silberberger. Houghton Mifflin Co., Boston, Mass., 1970.
- [14] Daisuke Tambara and Shigeru Yamagami. Tensor categories with fusion rules of self-duality for finite abelian groups. *J. Algebra*, 209(2):692–707, 1998.
- [15] Umberto Zannier. On the linear independence of roots of unity over finite extensions of  $\mathbf{Q}$ . *Acta Arith.*, 52(2):171–182, 1989.

*E-mail address:* `hannahlarson@college.harvard.edu`